Cyber Capability Development Centre (CCDC)

Proposed governance model

Prepared by: Douglas Wiemer

Contractor's Name and Address:
AEPOS Technologies Corporation
600-116 Albert Street Ottawa, Ontario K1P 5G3

PWGSC Contract Number: W7714-125420/001/ZM

Contract Scientific Authority:
Kathryn Perrett
Leader, Cyber Analytics and Tactics Group
Phone 613-993-5132

Contract Report
DRDC-RDDC-2014-C170
December 2013

Cyber Capability Development Centre (CCDC)

Proposed governance model

Douglas Wiemer

AEPOS Technologies Corporation

December 2013

Table of Contents

Table of Figures

List of Tables

1 Introduction

The Canadian Department of National Defence/Canadian Armed Forces (DND/CAF) currently lacks the ability and resources (both technological and personnel) to quickly evaluate and validate cyber operations concepts and solutions to counter the rapidly evolving cyber threat. Consequently, the Cyber Capability Development Centre (CCDC) is proposed as an agile and effective cyber Science and Technology (S&T) service capability for research, experimentation, test and evaluation, demonstration and training to support the needs of the DND/CAF and other departments across the Government of Canada.

Defence Research and Development Canada (DRDC) is uniquely positioned to establish the CCDC, creating Canada's leading national cyber operations S&T centre. DRDC has research specialists developing the next generation of tools for future cyber operations and information security practitioners supporting the current day-to-day operations of DRDC networks and systems. It is believed that the research and operations groups and DRDC in general would each gain from working more closely together. The intentional collaboration between these groups would help ground the Cyber Operations S&T Program while ensuring the network operators have access to the latest technologies and concepts to deal with current and future problems. Moreover, in addition to research networks and facilities, DRDC has access to the Defence Research Establishment network (DREnet), a corporate network that can be used as a live environment to advance cyber security S&T.

1.1 Purpose

The purpose of this document is to propose a governance structure for the CCDC and to present two implementation options with supporting information related to the benefits or drawbacks of each. This will support selection of the desired approach to establish the CCDC.

1.2 Scope

The scope of the CCDC Governance Model includes identification of the authority under which the CCDC is established, the vision and mission of the CCDC, services to be provided, as well as the supporting organizational structure, decision-making process, and implementation objectives. Further, the scope is limited to the examination of two alternate implementation models (dedicated management staff and assignment of management staff as secondary duties).

Supporting aspects required for the establishment and operation of the CCDC including infrastructure, facilities and technology are outside the scope of the CCDC Governance Model.

1.3 References

The following references were used in the development of this governance document:

- Cyber Security S&T Strategy (February 2011).
- CCDC Presentation, Cyber Group Retreat, DRDC Valcartier (September 2012).
- Cyber Range Summary Report (date unknown).
- Cyber Range Proposal v2.2 (date unknown).
- Cyber Capability Development Centre (CCDC) Science & Technology (S&T) Requirements, Logical Architecture & Reference Design v1.0, DRDC Ottawa CR 2013-057 (July 2013).
- CCDC Project Proposal (February 2013).
- Inria, "Description of Inria committees," http://www.inria.fr/en/institute/organisation/general-organization-chart (accessed 2 May 2013).

- Fraunhofer-Gesellschaft, “Structure and Organization of Fraunhofer-Gesellschaft,” http://www.fraunhofer.de/en/about-fraunhofer/structure-organization.html (accessed 2 May 2013).
- Interview with DETER Project Team (17 December 2012).
- Army Research Lab, “About ARL”, http://www.arl.army.mil/www/default.cfm?page=20 (accessed 2 May 2013).
- DARPA, “About”, http://www.darpa.mil/About.aspx (accessed 2 May 2013).
- Air Force Research Lab, “Welcome,” http://www.wpafb.af.mil/main/welcome.asp (accessed 2 May 2013).
- G. Hallingstad and L. Dandurand, “Communication and Information System Security Capability Breakdown, NATO Technical Report 2012/SPW008416/03 revision 4B (pre-release version), NCI Agency (8 February 2013).

2 Structure and governance (proposed)

2.1 Issuing authority

The CCDC is established as an organizational entity within DRDC under the authority of the Assistant Deputy Minister (Science & Technology) (ADM(S&T)) operating as Chief Executive Officer of DRDC.

2.2 Vision

The vision of the CCDC is to be Canada’s leading national cyber operations S&T centre by combining the knowledge of research, development and operational cyber experts and providing an environment to advance the cyber capability state-of-the-art.

2.3 Mission

The mission of the CCDC is to provide agile and effective cyber operations S&T services including research, experimentation, test and evaluation, demonstration, exercise and training services supporting the needs of the DND/CAF.

2.4 Objectives

The objectives of the CCDC, to be met through a combination of services and organization, are:

1. Provide leading cyber capability recommendations to the CAF resulting from cyber S&T outcomes validated and demonstrated in an off-line (contained) environment;
2. Advance cyber S&T outcomes through the synergistic effects of a multi-disciplinary team involving network management, cyber S&T research, and intelligence communities working together;
3. Counter the rapidly evolving and sophisticated threats through direct and agile development of defensive tools;
4. Develop and test cyber operations tactics and procedures through red-team exercises, having direct effects on CAF cyber capability development;
5. Support CAF cyber force generation activities through operational exercises and hands-on training;
6. Provide a test and evaluation facility for Canadian Industry interested in developing and deploying equipment for the CAF; and

7. Provide cyber-related trading commodities (knowledge, expertise, facilities, tools and techniques) that Canada can use to augment its contribution to the collective good of allied nations.

2.5 Services provided

To meet the identified Vision, Mission and Objectives, the following services are provided by the CCDC:

1. **Cyber capability requirements research:** Continuous S&T investigation of cyber requirements through analysis of the evolving cyber threat capabilities, identification of cyber capability deficiencies, and development and pursuit of advanced cyber capability programmes of work designed to counter the threat;
2. **Cyber incident and events forensics analysis:** Combined S&T and operational expert analysis of cyber incident and event information supporting root cause attribution, adversary capability analysis, impact assessment, and attack prediction leading to refinement of cyber capability requirements research and operational tools and tactics development;
3. **Cyber operations tools development, experimentation and deployment:** Development of cyber operations tools to meet cyber capability requirements and counter sophisticated cyber threats through rapid cycles of development, experimentation and deployment into operational environments;
4. **Cyber operations tactics and procedures development, experimentation and deployment:** Development of cyber tactics and procedures to meet cyber capability requirements and counter sophisticated cyber threats through rapid cycles of development, experimentation and deployment into operational environments;
5. **Cyber training and exercise support:** Hosted hands-on cyber tools, tactics and procedure training supported by cyber operations exercise planning, attack and defensive team coordination, outcomes evaluation and technical environment support; and
6. **Technical Environment:** The infrastructure supporting the development, experimentation, training and exercise needs of services provided by the CCDC.

2.6 Capability development description

The NATO Communications and Information Agency (NCI Agency) has developed the Communication and Information System (CIS) Security Capability Breakdown[1]. The CIS Security Capability Breakdown provides a common taxonomy and structured reference to describe CIS Security Capabilities for NATO and the participating nations. To add clarity to the benefits that are anticipated from the CCDC, it may be helpful to describe the capability development areas directly supported by the CCDC. It is anticipated that the following S&T related CIS security capability areas will benefit from establishing the CCDC within DRDC:

- **Govern CIS security:** The ability to establish strategic direction for CIS security, establish policies to secure the CIS and the information it handles, including standard approaches, minimum and desirable security requirements, definition of metrics, definition of information protection and release policies, definition of CIS security metadata, and finally, to audit CIS security for the purpose of accountability;
- **Design and Implement CIS security:** The ability to manage CIS security requirements, and design, implement, verify, and validate CIS security, to ensure that the implemented CIS is built

[1] G. Hallingstad and L. Dandurand, "Communication and Information System Security Capability Breakdown, NATO Technical Report 2012/SPW008416/03 revision 4B (pre-release version), NCI Agency, 8 February 2013.

in an efficient and adaptive manner, meets the security requirements and functions correctly, and is aligned with high-level direction and guidance;

- **Operate CIS security:** The ability to detect, prevent, and mitigate malicious activities and faults, to assess risk, damage, and attacks and faults, to recover from attacks and faults, decide on response, as well as to manage service level agreements;
- **Enable CIS security improvements:** The ability to assess the effectiveness and efficiency of CIS security, recommend improvement to CIS security, and advance CIS security through research; and
- **Educate, train, and exercise personnel on CIS security:** The ability to improve the effectiveness of individuals (e.g., CIS designers, implementers, users, operators, and risk owners) in directing and guiding CIS security, managing trustworthiness, managing CIS security information, designing and implementing CIS security, operating CIS security, and securing infrastructure critical to the CIS.

2.7 General organizational structure

This section provides a general description of the proposed organizational structure and relationships of the CCDC. Additional detail concerning the roles and responsibilities is provided in the next section. In this section, there is no particular determination of whether the roles and responsibilities are to be provided by dedicated management staff or as duties within the existing S&T Programs of DRDC.

The proposed organizational structure of the CCDC is illustrated in Figure 1. The non-management personnel within the CCDC are staffed from the Cyber Operations S&T Program of DRDC (across Research Centres including Ottawa, Valcartier, and the Centre for Operations Research and Analysis (CORA)) as well as personnel from DREnet Operations.

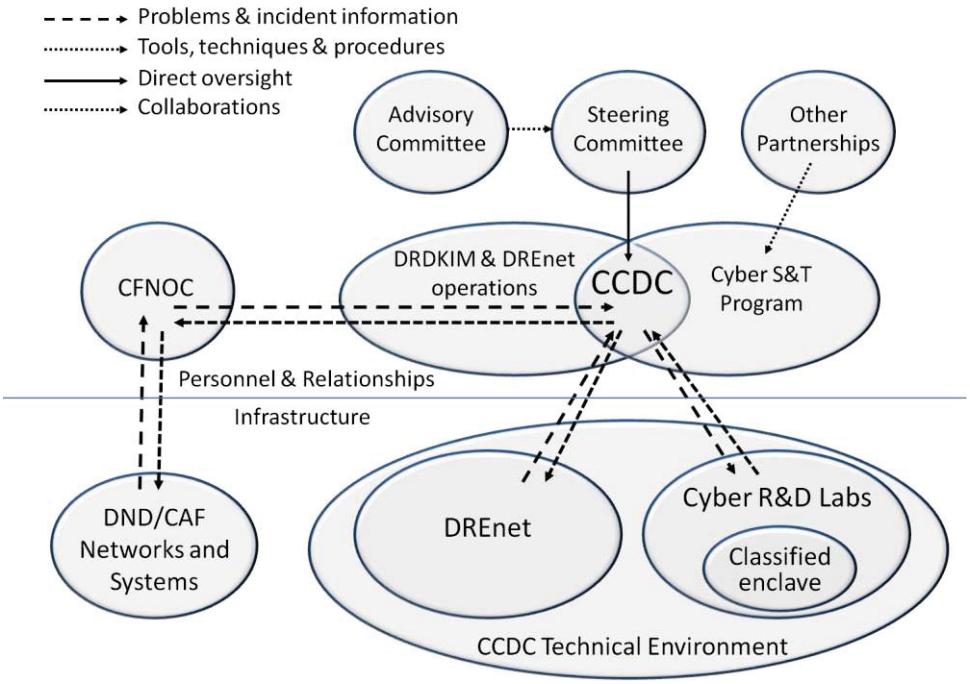

Figure 1: CCDC organization and infrastructure relationships

This structure takes advantage of the cooperative participation of personnel and resources from both the cyber research and operations communities. The activities of the CCDC are directed by a Steering Committee, co-chaired by Director General S&T Joint Force Development (DGSTJFD) and Director General Cyber (DG Cyber). The Steering Committee includes representation from across the cyber stakeholder community of DND. A collaborative relationship is maintained between the Steering Committee and the Advisory Committee. The Advisory Committee is established by the Steering Committee to receive advice from a panel of experts representing industry, academia, allies and other government departments. Additional influence will also be received by the Cyber Operations S&T Program through other partnerships that may be established on a project-by-project basis.

The Canadian Forces Network Operations Centre (CFNOC) is anticipated to be a primary operational beneficiary of the CCDC. Therefore, a formalized working relationship between the CCDC and the CFNOC should be established and maintained. The mission of the CFNOC is "to gain and maintain cyber superiority within the CAF cyber environment in order to assure friendly-force freedom of action." As such, the CFNOC has the ongoing responsibility for maintaining cyber situation awareness of DND/CAF networks and responding to cyber incidents whether sourced from an adversary or otherwise. Due to the formal relationship between the CFNOC and the CCDC, information pertaining to cyber problems and incidents can be passed to the CCDC such that the CCDC R&D Labs can be used to conduct forensic experiments supporting root cause analysis (including adversary attribution) and development of tools, techniques and procedures to aid CFNOC operations support of DND/CAF networks and systems.

In a similar way, DREnet operations staff has the ongoing responsibility for the cyber security posture of the DREnet. The organizational relationship between DREnet operations and staff of the Cyber Operations S&T Program provides an environment in which information pertaining to cyber issues on the DREnet can be passed to the CCDC, such that the CCDC R&D Labs can be used for analysis and development of tools, techniques and procedures for deployment and use on the DREnet.

2.7.1 Roles and responsibilities

This section provides additional detail concerning the roles and responsibilities of the various organizational bodies relative to the CCDC.

2.7.1.1 Steering Committee

The Steering Committee is responsible for the direct oversight and governance of the CCDC. The Steering Committee is co-chaired by the DRDC DGSTJFD and DG Cyber and includes representatives from other DND/CAF cyber stakeholders. The Steering Committee has the following responsibilities:

- Deliberating on measures concerning the CCDC organization and operations;
- Considering and recommending research priorities presented by its members, by the Advisory Committee or by CCDC staff;
- Review and endorsement for approval of the CCDC Program of Work;
- Review and endorsement for approval of the CCDC operating budget;
- Advising the CCDC Lead on research priorities;
- Providing the CCDC Lead with sufficient guidance, staff assistance and delegated authority for the proper conduct of research priorities;
- Reviewing recommended proposals to change research priorities;
- Ensuring that contingency funds are available for support to analysis of problems and incidents raised by CFNOC or DREnet operations; and
- Monitoring and reviewing research progress and outcomes.

The Steering Committee consists of representatives from the following organizations:

- Director General Science & Technology Joint Force Development (DGSTJFD);
- Director General Science & Technology Centre Operations (DGSTCO);
- Defence Research and Development Knowledge Information Management (DRDKIM);
- Director General – Cyber (DG Cyber);
- Commanding Officer Canadian Forces Network Operations Centre (CO CFNOC)
- Canadian Forces Information Operations Group (CFIOG) – Signals Intelligence (SIGINT);
- DND/CAF Joint Staff Intelligence (J2 STI);
- Defence Research and Development Canada (DRDC) – Centre for Security Sciences (CSS);
- Defence Research and Development Canada (DRDC) – Centre for Operational Research and Analysis (CORA);
- Communications Security Establishment Canada (CSEC);
- Royal Military College of Canada (RMCC); and
- CCDC Lead – non-voting member.

2.7.1.2 Steering Committee Co-Chairs

The Co-Chairs of the Steering Committee are responsible for:

- Chairing the Steering Committee and overseeing the implementation of the CCDC Program of Work;
- Coordinating the efforts of the Steering Committee to provide relevant guidance to the CCDC Lead in the development and review of the proposed CCDC Program of Work;
- Resolving conflicting project priorities between members of the Steering Committee;
- Controlling the expenditure of contingency funds and ensuring that such expenditure is consistent with the need for analysis of immediate operational problems and incidents critical to the ongoing operation of DND/CAF networks and systems;
- Ensuring that progress is made towards the approved CCDC Program of Work objectives, and that corrective action is taken whenever necessary; and
- Ensuring compliance with appropriate management practices, consistent with the methods and procedures for the management of projects in DND.

2.7.1.3 CCDC Lead

Reporting to the Steering Committee, the CCDC Lead is responsible for:

- Preparing the proposed CCDC Program of Work in collaboration with the DND/CAF cyber stakeholder community;
- Identifying the resources required by the proposed CCDC Program of Work;
- Ensuring that all approved Program of Work objectives are met, within the assigned resources;
- Managing and administering project activities according to assigned priorities and within the allocated budget;
- In consultation with the Steering Committee, resolving conflicts between assigned project priorities;
- Ensuring that Intellectual Property (IP) resulting from project activities is identified and appropriately documented;
- Collaborating with the CFNOC and DREnet Operations in the analysis of problems and incidents raised;

- Collaborating with the CFNOC and DREnet Operations in the deployment of cyber tools, techniques and procedures developed by the CCDC;
- Collaborating with other partners to meet Program of Work objectives; and
- Advising the Steering Committee of any significant developments which may affect the ability to meet project priorities and recommending corrective actions that should be taken.

2.7.1.4 Scientific Team Lead

Reporting to the CCDC Lead, the CCDC Scientific Team Lead is responsible for:

- Assisting the CCDC Lead in developing the proposed CCDC scientific Program of Work;
- Establishing or validating the scientific and technological objectives of the proposed CCDC Program of Work;
- Assisting the CCDC Lead in the development of work packages forming the proposed CCDC scientific Program of Work;
- Ensuring that all approved scientific Program of Work objectives are met, within the assigned resources;
- Managing and administering scientific project activities according to assigned priorities and within the allocated budget;
- Identifying to the CCDC Lead any conflicts between assigned project priorities;
- Ensuring that Intellectual Property (IP) resulting from project activities is identified and appropriately documented;
- Collaborating with the CFNOC and DREnet Operations in the analysis of problems and incidents raised;
- Collaborating with the CFNOC and DREnet Operations in the deployment of cyber tools, techniques and procedures developed by the CCDC;
- Collaborating with other partners to meet Program of Work objectives; and
- Advising the CCDC Lead of any significant developments which may affect the ability to meet project priorities and recommending corrective actions that should be taken.

2.7.2 Training and Exercise Team Lead

Reporting to the CCDC Lead, the CCDC Training and Exercise Team Lead is responsible for:

- Assisting the CCDC Lead in developing the proposed CCDC training and exercise Program of Work;
- Establishing or validating the training and exercise objectives of the proposed CCDC Program of Work;
- Assisting the CCDC Lead in the development of work packages forming the proposed CCDC training and exercise Program of Work;
- Ensuring that all approved training and exercise Program of Work objectives are met, within the assigned resources;
- Managing and administering training and exercise project activities according to assigned priorities and within the allocated budget;
- Identifying to the CCDC Lead conflicts between assigned project priorities;
- Ensuring that Intellectual Property (IP) resulting from project activities is identified and appropriately documented;
- Collaborating with the CFNOC and DREnet Operations in the preparation and conduct of training and exercise activities;

- Collaborating with the CFNOC and DREnet Operations in the selection of cyber tools, techniques and procedures to be included in training and exercise activities;
- Collaborating with other partners to meet Program of Work objectives; and
- Advising the CCDC Lead of any significant developments which may affect the ability to meet project priorities and recommending corrective actions that should be taken.

2.7.2.1 Advisory Committee

The Advisory Committee is responsible for providing advice and guidance to the Steering Committee. The Advisory Committee is made up of representatives from research institutes, academia, industry, other government departments, and allies who have been invited by the Steering Committee to participate due to the relevance of invitee expertise to the ongoing DND/CAF problems of cyber security. Membership in the Advisory Committee is reviewed by the Steering Committee on a yearly basis. The Advisory Committee has the following responsibilities:

- Provide relevant guidance to the Steering Committee concerning the evolution of cyber threats and the state-of-the-art for cyber tools, techniques and procedures to aid in the development of the CCDC Program of Work;
- Supporting the Steering Committee in the review of CCDC research outcomes; and
- Supporting the Steering Committee in the review of CCDC vision, mission, objectives, services organisation, and project priorities.

The Advisory Committee consists of representatives from the following organizations:

- Public Safety Canada;
- Communications Research Centre Canada;
- North Atlantic Treaty Organization;
- United States Department of Homeland Security (DHS);
- One or more of the United States Air Force Research Labs, Army Research Labs or Navy Research Labs;
- Representatives from one or more member nations of the 5-eyes community;
- Academic institutes based on relevance to ongoing CCDC Program of Work activities;
- Research institutes based on relevance to ongoing CCDC Program of Work activities; and
- Industry representatives based on relevance to ongoing CCDC Program of Work activities.

2.7.2.2 Advisory Committee Chair

The Chair of the Advisory Committee is elected on a yearly basis from the membership of the Advisory Committee by a simple majority vote. The Chair of the Advisory Committee is responsible for:

- Chairing the Advisory Committee and coordinating the efforts of the Advisory Committee to provide relevant guidance to the Steering Committee concerning the evolution of cyber threats and the state-of-the-art for cyber tools, techniques and procedures to aid in the development of the CCDC Program of Work; and
- Supporting the Steering Committee in the review of CCDC research outcomes.

2.8 Other partnerships

The CCDC establishes other partnerships with members of the cyber security research, academic and industrial community and formalized through a memorandum of understanding (MOU) based on a mutual set of priorities in keeping with the CCDC Program of Work. The MOU describes a specific

research or training activity with a defined scope, objective, duration and cost. In addition, the Steering Committee ensures that the collaboration is consistent with the approved CCDC Program of Work.

The process for establishing partnerships is organized in the following manner:

1. The **preparation phase** aims to work with the potential partner to assess the interest and scope of collaboration and to identify the CCDC resources whose work packages and expertise match the scientific and technological priorities of the proposed collaboration.
2. The **negotiation phase** involves establishing the methods and the content of the partnership and leads to the signing of the MOU. At this point, all of the aspects associated with the definition and exploitation of intellectual property, the system for publications, and the governance of the MOU are reviewed and validated by the CCDC Steering Committee and DRDC legal department before the CCDC Lead signs the MOU.
3. The **implementation phase** involves operationally implementing the activities defined in the MOU, under the authority of an assigned scientific authority designated for his or her particular skills relevant to the MOU.

2.9 Stakeholder involvement

In order for the DND/CAF to receive the most benefit from the CCDC, it is extremely important that CCDC activities be actively coordinated with the stakeholder community. It is for this reason that the CCDC itself is co-chaired by both DRDC and DG Cyber. As noted above, the proposed CCDC Program of Work is prepared by the CCDC Lead in collaboration with the DND/CAF cyber stakeholder community. Regular meetings between the CCDC Lead, Scientific Lead and Training Lead; personnel from CFNOC and DRDKIM; and other stakeholders are essential.

However, stakeholder involvement should not be considered to mean that stakeholders determine the CCDC Program of Work. Sometimes, operational stakeholders may become too focused on near term operational issues they may not have sufficient visibility into future requirements and potential capability development. The CCDC is anticipated to be Canada's leading national cyber operations S&T centre. As such, the CCDC itself should be in a position to lead the recommendations and development of the Program of Work. Similarly, the CCDC personnel, being drawn from both scientific and operational communities, should already have significant insight into the operational demands.

2.10 Decision-making responsibility

The CCDC is established under the authority of the ADM(S&T) operating as Chief Executive Officer of DRDC. Consequently, the final decision-making authority for the CCDC rests with the ADM(S&T) who delegates the management responsibility to the DGSTJFD. As such, DGSTJFD has final decision-making responsibility concerning the CCDC Program of Work, operating budget, research priorities, etc. These decisions are taken in full consideration of the recommendations from the CCDC Lead, endorsements provided by the CCDC Steering Committee, and advice received from the CCDC Advisory Committee. The responsibility for the day-to-day management and implementation of these decisions is assigned to the CCDC Lead.

3 Implementation objectives

The project plan is outlined below. Note that the detailed project progression beyond Phase I will depend on the results of the options analysis.

3.1 Current and completed efforts

Several efforts have been completed, including S&T and stakeholder requirements gathering, a logical architecture design, and the development of a potential governance model. Efforts that are currently underway include delivering a Terms of Reference (including processes and procedures), a high-level multi-phase architecture and deployment strategy, a DETER-compatible test-bed installation at DRDC Ottawa Research Centre (with potential for a future federated architecture across multiple sites), and an options analysis for later phases of the CCDC.

3.2 Phase I

The CCDC organization will be formalized within DRDC, the Steering Committee will be established and CCDC positions (CCDC Lead, Scientific Team Lead, Training and Exercise Team Lead) created and an initial head count allocated. Aside from the CCDC Lead and Team Lead positions, all other positions within the CCDC are established as matrix positions assigned from the DREnet Operations and Cyber Operations S&T Program staffs. Activities to develop the CCDC Program of Work will commence with a target to present a four-year proposed CCDC Program of Work to the Steering Committee for approval. The members of the Steering Committee will propose, select and invite representatives to the Advisory Committee.

An S&T research capability will be implemented, including an isolated virtualization-based experimental test-bed to satisfy the near-term needs of DRDC cyber S&T specialists (Phase I architecture implementation). Testing, documentation, and training will be completed for the DETER component of the facility. The goals are to develop a passive lab capability – to take stored network and system (N&S) data and examine their contents efficiently, and an active lab capability – to replay data recovered from the packet logs of events using intrusion detection systems (IDS) or similar devices.

3.3 Phase II

The CCDC will commence activities associated with the approved CCDC Program of Work. Additional resources will be assigned from DREnet Operations and Cyber Operations S&T Program as required to fulfill the approved Program of Work. Members of the CCDC will begin identification of possible collaboration partners and proposing these to the Steering Committee for approval.

Real data integration will be provided, with the ability to incorporate a live data feed from the DREnet. The goal is to create a realistic battle environment through the addition of real-time data from a live system. Forensic anomaly detection capabilities will allow for the investigation of sophisticated cyber threats. Interactive capabilities will also be provided for enhanced cyber S&T demonstrations, red-teaming exercises, and computer network operations training for DRDC and the CAF (Phase II implementation).

3.4 Phase III

Collaborative cyber S&T capabilities will enhance S&T development and testing across distributed partner organizations (Phase III implementation). Expanded sensing capabilities will also extend S&T researchers' ability to sense the test network both passively and actively.

4 Governance staffing options

This section considers implementation options for the governance implementation of the CCDC. Since the governance model is structured to leverage the existing DRDC DGSTJFD structure for senior

management governance, these options focus on the staffing of the CCDC Lead, Scientific Team Lead and Training and Exercise Team Lead positions. The two options to be considered include:

1. Use of dedicated staff; and
2. CCDC roles assigned to existing cyber S&T positions.

The comparison of the two options is provided in Table 1. A set of criteria is included in the table and each staffing option is evaluated against this criteria. A generalized rating of "Pro" or "Con" is assigned to each evaluation.

Table 1: Evaluation of options for CCDC staffing

Criteria ID	Criteria	Use of dedicated staff	Assigned roles to existing cyber S&T positions
1	Promotion of and focus on CCDC goals and objectives	**(Rating: Pro)** Dedicated personnel have all their attention applied to the activities of the CCDC. As such, their ability to promote and focus on the CCDC goals and objectives is not distracted by other roles and responsibilities.	**(Rating: Con)** When CCDC roles and responsibilities are assigned as additional duties to existing cyber S&T staff, their attention may be distracted. Consequently, there will be a risk that their ability to promote and focus on CCDC goals and objectives will be hindered.
2	Adaptability to CCDC changing priorities	**(Rating: Pro)** Similar to Criteria ID #1 above, dedicated personnel have all their attention applied to the activities of the CCDC. As such, their ability to ability to adapt to changing priorities of the CCDC is not hindered by other roles and responsibilities.	**(Rating: Con)** Similar to Criteria ID #1 above, when CCDC roles and responsibilities are assigned as additional duties to existing cyber S&T staff, their ability to adapt to changing priorities of the CCDC may be hindered by other roles and responsibilities.
3	Impact on other cyber S&T activities	**(Rating: Pro)** Use of dedicated staff ensures CCDC duties will not adversely impact other cyber S&T activities.	**(Rating: Con)** Assignment of CCDC duties to existing cyber S&T staff may adversely impact other cyber S&T activities. Staff may not be able to manage the additional workload.
4	Staffing Costs	**(Rating: Con)** Use of dedicated staff introduces costs associated with at least 3 new staff (CCDC Lead, Scientific Team Lead and Training and Exercise Team Lead positions).	**(Rating: Pro)** Having CCDC roles and responsibilities assigned to existing cyber S&T positions ensures no additional staffing costs.

From the above table, and assuming there is an equal weighting to all criteria, having dedicated staff is in the best interests of the success of the CCDC. Dedicated staff will have the best opportunity to promote and achieve the objectives and goals of the CCDC. However, it is also recognized that overall costs may be a deciding factor. In this case, the cost of additional positions may prevent the use of dedicated staff.

5 Conclusions

The Canadian DND/CAF currently lacks the ability and resources (technological and personnel) to quickly evaluate and validate cyber operations concepts and solutions to counter the rapidly evolving cyber threat. Consequently, the CCDC is proposed as an agile and effective cyber S&T service capability for research, experimentation, test and evaluation, demonstration and training to support the needs of the DND/CAF and other departments across the Government of Canada.

This document proposes a CCDC governance model. The model incorporates concepts from successful research organizations indicated in the document references, while accounting for the structure of DRDC and its relationship to the DND/CAF. The proposed governance model includes the following:

1. Governance led by a Steering Committee that is co-chaired by DGSTJFD and DG Cyber;
2. Involvement of stakeholders on the Steering Committee identified from across the DND/CAF;
3. Participation and guidance received from an Advisory Committee representing perspectives from other national and international defence, government, academic, research and industry organizations;
4. Identification of specific roles and responsibilities for key leadership positions in the CCDC including the CCDC Lead, Scientific Team Lead and Training and Exercise Team Lead.

This document also provides some high level evaluation of two staffing options for the CCDC key leadership positions. Assuming there is an equal weighting to all criteria, it is recommended that the CCDC have assigned dedicated staff positions instead of assigning CCDC roles and responsibilities to existing Cyber Operations S&T Program positions. However, it is also recognized that overall costs may be a deciding factor. In this case, the cost of additional positions may prevent the use of dedicated staff.

Glossary

ADM(S&T)	Assistant Deputy Minister (Science and Technology)
CAF	Canadian Armed Forces
CCDC	Cyber Capability Development Centre
CFIOG	Canadian Forces Information Operations Group
CFNOC	Canadian Forces Network Operations Centre
CIS	Communication and Information System
CO	Commanding Officer
CORA	Centre for Operational Research and Analysis
CSEC	Communications Security Establishment Canada
CSS	Centre for Security Sciences
DETER	Cyber-Defence technology Experimental Research
DG Cyber	Director General Cyber
DGSTCO	Director General S&T Centre Operations
DGSTJFD	Director General S&T Joint Force Development
DHS	(US) Department of Homeland Security
DND	Department of National Defence
DRDC	Defence Research & Development Canada
DRDKIM	Defence Research and Development Knowledge Information Management
DREnet	Defence Research Establishment Network
IP	Intellectual Property
MOU	Memorandum of Understanding
NATO	North Atlantic Treaty Organization
NCI	NATO Communications and Information
R&D	Research and Development
RMCC	Royal Military College of Canada
S&T	Science and Technology
SIGINT	Signals Intelligence